



Homeland  
Security

# Daily Open Source Infrastructure Report

## 6 July 2012

### Top Stories

- Six days after violent storms hit the United States, more than 500,000 homes and businesses remained without power from Ohio to Virginia as a heat wave baked much of the nation July 5. – *Reuters* (See item [1](#))
- A new version of the Sykipot trojan is targeting unsuspecting computer users, including attacks on attendees of an international aerospace conference, according to researchers. – *Threatpost* (See item [13](#))
- Lemont, Illinois police suspect someone hacked into the village's tornado siren system, causing all seven sirens to sound for about 30 minutes, the police chief said. – *Chicago Tribune* (See item [50](#))
- For the second time in weeks, Symantec security researchers uncovered a computer worm that forces network printers at organizations to suddenly print reams of useless data. – *IDG News Service* (See item [58](#))

---

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

#### SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

#### SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

#### FEDERAL and STATE

- [Government Facilities](#)
  - [Emergency Services](#)
  - [National Monuments and Icons](#)
-

## **Energy Sector**

1. *July 5, Reuters* – (National) **500,000 customers still without power after storms.** Six days after violent storms hit the United States, more than 500,000 homes and businesses remained without power from Ohio to Virginia as a heat wave baked much of the nation July 5. Nearly a third of electricity customers in West Virginia, home to 1.9 million people, were without power, making it the hardest hit State. Utilities warned that some people could be without power for the rest of the week in the worst-hit areas. Temperatures in Charleston were expected to reach 95 degrees and top 100 degrees July 6-7. The storms crossed the eastern United States with heavy rain, hail and winds reaching 80 miles per hour June 29, leaving more than 4 million homes and businesses without power, and the record heat that followed has killed at least 23 people.  
Source: <http://www.reuters.com/article/2012/07/05/us-usa-weather-power-idUSBRE8640QK20120705>
2. *July 3, Raleigh News Observer* – (North Carolina) **At least two injured in explosion at Sanford oil plant.** At least two people suffered injuries July 3 following an explosion at an oil plant in Sanford, North Carolina, fire officials reported. The explosion occurred at Noble Oil Services authorities reported. Firefighters with the Northview Rural Fire Department responded. A spokeswoman with the company said that the incident was under control after several hours.  
Source: <http://www.newsobserver.com/2012/07/03/2177495/firefighters-respond-to-late-morning.html>
3. *July 3, Evansville Courier-Press* – (Kentucky) **U.S. 41-Alternate reopens in Webster County after lightning strike fire.** Kentucky transportation officials said U.S. 41-Alternate was reopened in Webster County, Kentucky, after a lightning strike ignited an oil well tank fire. The Kentucky Transportation Cabinet said the tanks burst into flames after being hit by lightning July 2. The lid from one of the tanks was blown onto the nearby highway. The well is between Dixon and Providence. Two other tanks were burning when firefighters arrived. A representative of the well operator said a tanker truck had recently pumped oil from the tanks, lessening the fire hazard. Heavy rain that accompanied the storms helped keep the flames from spreading. The explosion and fire also damaged some power lines in the area, knocking out service to some customers.  
Source: <http://www.courierpress.com/news/2012/jul/03/explosion-closes-us-41-alternate-webster-county/>
4. *July 2, KZTV 10 Corpus Christi* – (Texas) **Copper theft leaves thousands without power.** Thousands of people were left without power after copper thieves hit an American Electric Power (AEP) substation in Corpus Christi, Texas, July 2. An AEP spokesman said the wire stolen was the ground wire that lead up to the transformers. Because of the location of the wires, they had to shut off power for about 4,100 customers so they could repair it. An AEP spokesperson said the substations are already fairly secure, but AEP will look at how the thieves got in to see if any more changes must be made.  
Source: <http://www.kztv10.com/news/copper-theft-leave-thousands-without-power/>

For more stories, see items [23](#) and [25](#)

[\[Return to top\]](#)

## **Chemical Industry Sector**

5. *July 3, Dearborn County Register* – (Ohio; Indiana) **Chemical spill causes mess and aggravation.** U.S. 50 at Lawrenceburg Road in Elizabethtown, Ohio, was completely shut down near the State line's border with Indiana, July 2 after a drum containing a corrosive substance leaked nearly all of its 55 gallons off of a truck owned by Midwest Environmental Services, West Chester, the Whitewater Township fire chief said. The substance, called Sodium Mbt, 50 percent solution, is a corrosive chemical that can burn the respiratory system and cause eye and skin irritation. The Whitewater Township Fire Department, Miami Township Fire Department, Harrison Fire Department's HAZMAT Unit, and the Hamilton County Sheriff's Department responded to the scene, which took about 4.5 hours to completely clean up. Traffic was completely shut down in both directions for about 1.5 hours.

Source:

[http://www.thedcregister.com/index.php?option=com\\_content&view=article&id=4094:chemical-spill-causes-mess-and-aggravation&catid=1:latest-news&Itemid=44](http://www.thedcregister.com/index.php?option=com_content&view=article&id=4094:chemical-spill-causes-mess-and-aggravation&catid=1:latest-news&Itemid=44)

6. *July 2, U.S. Food and Drug Administration* – (National) **FDA announces the voluntary removal by industry of certain perfluorinated greaseproofing agents from the marketplace.** The U.S. Food and Drug Administration (FDA) announced July 2, five perfluorinated substances used as greaseproofing agents were voluntarily removed from interstate commerce by their manufacturers. After recent studies raised safety concerns with one type of perfluorinated chemical, known as C8, FDA initiated a comprehensive review of the available data. The decision by the chemical manufacturers, including BASF Corporation, E. I. DuPont de Nemours & Co, and Clariant, means the affected products will no longer be sold for application on paper or paperboard intended for food contact use. This commitment is noted on the FDA's Inventory of Effective Food Contact Substance (FCS) Notifications. The agency will also conduct a market survey of food packaging to ensure these compounds are no longer used in material that comes in contact with human or animal food.

Source: <http://www.fda.gov/Food/NewsEvents/ConstituentUpdates/ucm309925.htm>

For another story, see item [14](#)

[\[Return to top\]](#)

## **Nuclear Reactors, Materials and Waste Sector**

7. *July 5, Bloomberg* – (International) **Fukushima disaster was man-made, investigation finds.** The Fukushima nuclear disaster was the result of a mix of “man-made” factors, including regulators who failed to provide adequate prevention and a government lacking commitment to protect the public, said a report from an independent Japanese parliamentary investigation, Bloomberg reported July 5. The

report, the harshest critique yet of the government and Tokyo Electric Power Co., also said the investigation can not rule out that the earthquake March 11, 2011, caused damage to the Fukushima Dai-Ichi No. 1 reactor and safety equipment. This was a departure from other reports that concluded the reactors withstood the earthquake only to be disabled when the ensuing tsunami hit the plant. This finding may have implications for all of Japan's nuclear plant operators if it leads to tougher earthquake-resistance standards. If the Fukushima reactor had already been crippled by the quake when the tsunami hit, it would force regulators to reconsider the seismic criteria that all of Japan's plants must live up to, their so-called design basis, said a professor of civil engineering at the University of Southern California.

Source: <http://www.bloomberg.com/news/2012-07-05/fukushima-nuclear-disaster-was-man-made-investigation-rules.html>

[\[Return to top\]](#)

## **Critical Manufacturing Sector**

8. *July 5, U.S. Department of Labor* – (New York) **U.S. Labor Department's OSHA cites Long Island, NY, machine shop for failing to correct previously cited hazards.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) July 5 cited Simtek Inc. for alleged repeat and serious violations of workplace safety standards as well as failing to correct eight hazardous conditions cited during a 2011 OSHA inspection that was prompted by a worker injury. The Amityville, New York metal fabrication shop faced \$138,765 in proposed fines based on the latest inspection for new, recurring, and uncorrected hazards. OSHA originally cited Simtek in June 2011 for 20 violations of workplace safety standards, including missing or incomplete energy control procedures and various electrical hazards. The agency initiated a follow-up inspection in January to verify whether the cited hazards had been abated. Inspectors found Simtek still had not developed and put into use energy control procedures to lock out machines' power sources to prevent them from starting up during maintenance, nor had the company provided training and tools to workers who perform the maintenance. It also had failed to correct several electrical hazards.

Source:

[http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=22629](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22629)

9. *July 3, Detroit News* – (National) **Volvo to pay \$1.5M U.S. fine over late recalls.** Volvo Cars North America will pay \$1.5 million in fines to settle claims that the company failed to report safety defects in a timely manner in seven recall campaigns since 2010, Detroit News reported July 3. The company apologized for the delays and said it would work to improve its recall procedures and emphasized that there were no injuries or crashes connected to any of the recalls. The National Highway Traffic Safety Administration said that Volvo will pay civil fines for failing to conduct recall campaigns in a timely fashion — including six in 2010, and one in 2012.

Source:

[http://www.detroitnews.com/article/20120703/AUTO0104/207030388/1121/AUTO01/Volvo-to-pay-\\$1.5M-U.S.-fine-over-late-recalls](http://www.detroitnews.com/article/20120703/AUTO0104/207030388/1121/AUTO01/Volvo-to-pay-$1.5M-U.S.-fine-over-late-recalls)

10. *July 3, U.S. Consumer Product Safety Commission* – (National) **Innovage recalls Discovery Kids lamps due to fire and burn hazards.** The U.S. Consumer Product Safety Commission, in cooperation with Innovage LLC, July 3 announced a voluntary recall of about 300,000 Discovery Kids Animated Marine and Safari Lamps. Consumers should stop using recalled products immediately unless otherwise instructed. The placement of internal wires near the circuit board can cause electrical short-circuiting and sparking, posing a fire and a burn hazard to consumers. Innovage has received 11 reports of short circuiting. This includes three reports of lamps catching fire, which led to property damage. The lamps were sold at Bed Bath and Beyond, Bonton, JCPenney, Kohls, Office Max, and Toys "R" Us stores nationwide as well as through online retailers from June 2010 through March 2012.  
Source: <http://www.cpsc.gov/cpscpub/prerel/prhtml12/12215.html>

For another story, see item [13](#)

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

11. *July 5, Global Security Newswire* – (National) **Aging U.S. atomic shipping gear poses concern, auditors find.** The old age of the U.S. Energy Department's highly protected atomic-transport automobiles is one of "several" major hurdles faced by its Secure Transportation Office, the department's inspector general said in an assessment issued June 29. "Based on its own criteria, [the Secure Transportation Office's] entire fleet of armored tractors is beyond its operational life as of December 2011," the Knoxville News Sentinel quoted the department's auditors as saying in the analysis. U.S. nuclear-warhead sustainment efforts and transfers of arms production components are set to substantially boost the need for closely guarded atomic transports over the coming 84 months, the assessment states. The Secure Transportation Office has satisfied a majority of transfer needs to date, though, and its capabilities are projected to remain sufficient, according to the findings. Other concerns "include maintaining the reliability of existing equipment; ensuring that future federal agent overtime levels are consistent with safe operations; and, validating essential resource planning data," an assessment abstract states. "Accordingly, management attention is needed to address these challenges to reduce the risk that [the Secure Transportation Office] will be unable to meet its future mission requirements."  
Source: <http://www.nti.org/gsn/article/aging-us-atomic-shipping-gear-poses-concern-audit/>
12. *July 5, Associated Press* – (Virginia) **Chemical leak at Army ammo plant in Radford.** A key production line remained shut down at the Radford Army Ammunition plant in Radford, Virginia, after a chemical leak, the Associated Press reported July 5. The U.S. Army and plant operator had said after the July 1 incident that they expected operations to return to normal July 3, but that did not happen. An Army spokeswoman

told the Roanoke Times that officials were still reviewing the incident, and it could take several days. A spokesman for the plant operator said that by “normal,” officials meant the plant would be fully ready to meet customers’ needs July 3, and that was achieved. The Army previously said it has an inventory it can draw from in times of need. One employee was taken to a hospital for observation after exposure to fumes. Officials said he was released July 2.

Source: <http://www.newsleader.com/article/20120705/NEWS01/120705002/Chemical-leak-Army-ammo-plant-Radford>

13. *July 3, Threatpost* – (International) **New version of Sykipot trojan linked to targeted attacks on aerospace industry.** According to researchers at the security firm AlienVault, a new version of the Sykipot trojan is being pushed to unsuspecting users in a wave of online attacks, including targeted attacks on attendees of an international aerospace conference, Threatpost reported July 3. The attacks use exploits for recently disclosed security holes, such as Microsoft's Windows XML Core Services vulnerability first disclosed in June. The new Sykipot variant also uses a collection of recently registered Web domains to issue malicious attacks. Most were registered in the last month and are linked to the same yahoo.com e-mail address, AlienVault disclosed. At least one of the new domains was linked to targeted phishing-email attacks on attendees of the IEEE Aerospace Conference (the International Conference for Aerospace Experts, Academics, Military Personnel, and Industry Leaders), AlienVault said.

Source: [http://threatpost.com/en\\_us/blogs/new-version-sykipot-trojan-linked-targeted-attacks-aerospace-industry-070312](http://threatpost.com/en_us/blogs/new-version-sykipot-trojan-linked-targeted-attacks-aerospace-industry-070312)

14. *July 3, Pittsburgh Tribune-Review* – (Pennsylvania) **Fire at tear gas maker challenging.** A fire at a storage facility at Nonlethal Technologies in Indiana County, Pennsylvania, created heavy smoke and shut down an area road, July 3. The blaze caused the evacuation of 40 workers at the Black Lick Township manufacturer of tear gas, rubber batons and nonlethal munitions for law enforcement and the military. Firefighters from about a half-dozen departments battled the blaze in 30-minute shifts while emergency crews monitored air quality. The director of the Indiana County Emergency Management Agency said readings did not indicate any issues downwind. Route 286 was closed for about 5 hours. Nonlethal Technologies is composed of four buildings, apparently done by design “so if they have an incident like this, it doesn’t affect the” operation, the director said. The fire occurred at a wood-frame, metal-sided storage facility used for shipping and receiving in a back corner of the plant site, where chemicals are stored by type in cargo containers. Chemicals are manipulated in another building.

Source: <http://triblive.com/news/2145594-74/county-plant-route-286-indiana-gas-tear-fire-nonlethal-stutzman>

15. *June 28, Associated Press* – (International) **United Technologies, subsidiaries to pay \$75 million for sending parts for Chinese helicopter.** A division of United Technologies Corp. (UTC) pleaded guilty June 28 to crimes related to the illegal export of software U.S. officials said was used by China to develop the country’s first modern military attack helicopter. The subsidiary, Pratt & Whitney Canada Corp., Hartford,



Connecticut-based UTC; and another subsidiary along with UTC agreed to pay more than \$75 million in fines in connection with the export violations, and for providing misleading information to the U.S. government. The U.S. attorney for Connecticut said Pratt & Whitney Canada knowingly committed the violations because it wanted to become the exclusive supplier for a helicopter market in China with projected revenues of up to \$2 billion.

Source: [http://www.washingtonpost.com/business/technology/united-technologies-subsidiaries-to-pay-75-million-for-sending-parts-for-chinese-helicopter/2012/06/28/gJQAnCBb9V\\_story.html](http://www.washingtonpost.com/business/technology/united-technologies-subsidiaries-to-pay-75-million-for-sending-parts-for-chinese-helicopter/2012/06/28/gJQAnCBb9V_story.html)

[\[Return to top\]](#)

## **Banking and Finance Sector**

16. *July 5, Softpedia* – (International) **Fraud alert: ZeuS malware steals banking details via fake login pages.** Security experts from Threat Metrix and the United Kingdom's Action Fraud warned Internet users to be on the lookout for a new variant of the infamous Zeus malware that attempts to steal sensitive data by posing as genuine log-in pages, Softpedia reported July 5. The fraud starts with a normal log-in page, but once unsuspecting users enter their credentials, they are presented with a Web page that requests credit card information. In the case of social media sites, the victim is notified that by completing the form he can link his payment card to the account to make the acquisition of Facebook credits easier. This operation allegedly also offers enhanced security and even 20 percent cash back. The trojan is also able to adjust balances so victims are unaware of the fraudulent transactions. Customers of payment processors and companies from the retail industry are also at risk since most Web sites can be easily replicated, and for each situation the fraudsters can come up with apparently legitimate reasons for why the victim must provide credit card details.

Source: <http://news.softpedia.com/news/Fraud-Alert-ZeuS-Malware-Steals-Banking-Details-Via-Fake-Login-Pages-279372.shtml>

17. *July 5, IDG News Service* – (Maine; National) **Federal appeals court raps bank over shoddy online security.** Patco Construction Company of Sanford, Maine, may stand a greater chance of recovering some of the \$345,000 it lost in fraudulent wire transfers that it blamed on poor online banking practices of its bank after a federal appeals court found the bank's online security measures were not "commercially reasonable," IDG News Service reported July 5. The company sued Ocean Bank, now called People's United Bank, after fraudsters made six wire transfers using the Automated Clearing House (ACH) transfer system, amounting to more than \$588,000 in May 2009. About \$243,000 was recovered. In its decision, the appeals court cited a critical mistake made by Ocean Bank as ACH fraud had become more prevalent. In June 2008, Ocean Bank decided to initiate "challenge questions" for any transactions for its customers valued at more than \$1. Since the answers to the questions were displayed every time Patco made a transfer, this "increased the risk that such answers would be compromised by keyloggers or other malware that would capture that information for unauthorized uses," the ruling said. The court also found Ocean Bank was not monitoring its transactions for fraud, nor notifying customers before a suspicious transaction was

allowed to proceed, both capabilities it possessed with its security system.

Source:

[http://www.computerworld.com/s/article/9228796/Federal\\_appeals\\_court\\_raps\\_U.S.\\_bank\\_over\\_shoddy\\_online\\_security](http://www.computerworld.com/s/article/9228796/Federal_appeals_court_raps_U.S._bank_over_shoddy_online_security)

18. *July 3, Costa Mesa Daily Pilot* – (California; International) **Man convicted of credit card fraud.** A Los Angeles man arrested in Costa Mesa, California, in August 2011 was convicted of stealing credit cards from the elderly, and was part of a network including conspirators from the United Kingdom, the Costa Mesa Daily Pilot reported July 3. The man was convicted the week of June 25 of six felonies, including charges of aggravated identity theft, bank fraud, and credit card fraud. Police said the man tried to flee after an employee discovered the card used was stolen and called police, but was caught and taken into custody. Costa Mesa police contacted and worked with federal authorities, who prosecuted an overarching case. Federal authorities said the man took control of about a dozen credit cards in a conspiracy involving British members who would allegedly impersonate cardholders and ask for replacement credit cards to be sent to different southern California drop locations. The Britons told credit card companies they were traveling in Southern California and would be making large purchases, according to the Department of Justice. The convicted man and others picked up the new credit cards, and, using the fake IDs, tried to buy more than \$250,000 in luxury items.

Source: [http://articles.dailypilot.com/2012-07-03/news/tn-dpt-0704-ward-20120703\\_1\\_credit-card-impersonate-cardholders-costa-mesa-police](http://articles.dailypilot.com/2012-07-03/news/tn-dpt-0704-ward-20120703_1_credit-card-impersonate-cardholders-costa-mesa-police)

19. *July 3, Federal Bureau of Investigation* – (National; International) **Massachusetts man pleads guilty to \$6.9 million fraud scheme.** A Boxford, Massachusetts man pleaded guilty July 3 to engaging in a fraudulent foreign investment scheme that defrauded at least 20 victims of more than \$6.9 million. He pled guilty to one count of conspiracy to commit wire fraud. The man claimed to be the president of a business called Tracten Corporation, and from September 2005 through April 2008, he conspired with others to engage in a fraudulent scheme that required investors to pay a fee that would be used to secure large letters of credit through European financial institutions. Investors were told the initial payment was a commitment fee necessary to secure a multi-million-dollar letter of credit, and that they would receive a percentage monthly return on the total amount. He admitted that in 2005, he and another co-conspirator made multiple trips to Rome, Italy, to meet with bank officials to pitch the letter of credit program. Despite the bank's refusal to participate, the conspirators secured an Internet domain name to set up an e-mail account that would appear to come from a bank representative and created fraudulent bank letterhead that also appeared to come from the bank.

Source: <http://www.fbi.gov/washingtondc/press-releases/2012/massachusetts-man-pleads-guilty-to-6.9-million-fraud-scheme>

For another story, see item [51](#)

[\[Return to top\]](#)



## **Transportation Sector**

20. *July 5, Buffalo News* – (New York) **Fire destroys CSX train warehouse in Lovejoy.** Officials did not determine the cause of the July 3 fire at a train warehouse in the Lovejoy neighborhood in Buffalo, New York, though neighbors believe suspicious activity, and not holiday fireworks, could be to blame. A witness told Buffalo News July 4 that he saw black smoke near his Schiller Street garage and ran to the CSX Railroad building at Reiman and North Ogden streets, where he spotted a black pickup speeding from the parking lot. The estimated loss was \$100,000. CSX officials said they would work with fire officials to ensure the building is demolished promptly.  
Source: <http://www.buffalonews.com/city/communities/buffalo/article934829.ece>
21. *July 5, KNVX 15 Phoenix* – (Arizona) **Rain, floods damage cars and homes in Casa Grande.** Rains and floods affected many neighborhoods in southern Arizona, KNVX 15 Phoenix reported July 5. Wet weather filled dozens of homes with flood waters in and around Casa Grande. Residents of Arizona City said this is the third time in the past several years the area was flooded by monsoon rains. In other parts of Pinal County, several cars became stuck in washed out sections of road and had to be pulled out. Fast moving water ran across many streets. Dozens of roads were closed for safety precautions.  
Source: [http://www.abc15.com/dpp/news/region\\_central\\_southern\\_az/casa\\_grande/rain-and-floods-damage-cars-and-homes](http://www.abc15.com/dpp/news/region_central_southern_az/casa_grande/rain-and-floods-damage-cars-and-homes)
22. *July 5, San Francisco Chronicle* – (California) **Lanes open after Bay Bridge shooting snarls traffic.** All eastbound lanes were reopened on the Bay Bridge in San Francisco, after police shut them down for about 10 hours while investigating a shooting on the middle of the span July 5. California Highway Patrol (CHP) officers pursued a car across the bridge when the car stopped just past Yerba Buena Island and shots were fired, authorities said. A CHP spokesman said he did not know whether the gunfire came from police or the driver. He said the driver was treated for injuries related to the crash. The driver was arrested on suspicion of felony drunken driving and weapons charges, the CHP said.  
Source: <http://www.sfgate.com/crime/article/Bay-Bridge-shooting-closes-eastbound-lanes-3685602.php>
23. *July 4, Chicago Tribune* – (Illinois) **Train derails, bridge collapses near Northbrook-Glenview border.** A freight train hauling coal derailed on Union Pacific tracks near Willow Road and Shermer Avenue July 4 by the Northbrook-Glenview, Illinois border. Witnesses said the bridge overpass over Shermer Avenue collapsed in the accident. A Union Pacific spokesman said the derailment occurred as the train headed to a utility plant in Wisconsin from a coal mine in Wyoming. The train had three locomotive engines and 31 of its 138 train cars derailed, the spokesman said. About a third of the train had passed the 86-foot-long bridge before the derailment and the locomotives did not derail. A small fire that involved vegetation occurred. The spokesman said the tracks are only used by its freight lines. For about the next 24 hours

crews cleaned up the spilled coal and removed the train cars. The workers will use stone fill to close up the gap where the bridge was, and install temporary tracks to get the trains moving again through the area. The railroad will have to design and build a new bridge.

Source: [http://articles.chicagotribune.com/2012-07-04/news/chi-train-derails-in-near-northbrookglenview-border-20120704\\_1\\_train-cars-train-derails-freight-train](http://articles.chicagotribune.com/2012-07-04/news/chi-train-derails-in-near-northbrookglenview-border-20120704_1_train-cars-train-derails-freight-train)

24. *July 3, U.S. Attorney's Office Southern District of Massachusetts* – (New York; Massachusetts) **Revere woman charged with making false bomb threat to Jet Blue.** A Revere, Massachusetts woman was arrested July 3 after being charged in federal court for falsely reporting explosives were on board a JetBlue flight. The woman was charged July 2 in a criminal complaint with providing false information and threats relating information that a passenger on board a flight from Logan International Airport in Boston, to O'Hare International Airport in Chicago, was carrying explosives. As a result, the flight was diverted and forced to land in Buffalo, New York. It was later determined she and a passenger were involved in a personal dispute. If convicted, the woman faces up to 5 years in prison to be followed by 3 years of supervised release and a \$250,000 fine.

Source: <http://www.justice.gov/usao/ma/news/2012/July/MillerNicolecharge.html>

25. *July 3, Associated Press* – (Washington) **Cleaning up derailed coal in Franklin County town.** A coal train that derailed and spilled 31 cars of fuel caused a day's delay in rail traffic in Mesa, Washington, July 2. About 50 workers using heavy equipment worked to clear the Burlington Northern Santa Fe main line track, said a spokesman. They were able to put 1 car back on the track, but 30 were too badly damaged. About 30 trains a day move through the area, about 20 miles north of the Tri-Cities. About four a day are coal trains, the State said. The route is also used by the Portland-Chicago Amtrak. Priority trains were able to roll through the area on a siding by July 3, and the main line was to re-open later that day, the spokesman said. The 125-car train with 4 locomotives was carrying coal from the Powder Basin in Wyoming to an export terminal at Delta, British Columbia. Canada.

Source: <http://www.thenewstribune.com/2012/07/02/2202734/coal-train-derails-in-columbia.html>

For more stories, see items [1](#), [3](#), [5](#), [14](#), [35](#), [42](#), and [71](#)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

26. *July 5, New Bedford Standard-Times* – (Massachusetts) **3 in Fall River charged with damaging mailboxes with explosives.** Three men were arrested July 3 on charges of using explosives to damage numerous mailboxes in Fall River, Massachusetts, after an investigation that included the police use of YouTube videos. The three men were charged with numerous counts of throwing/placing/exploding explosives, and malicious destruction of property over \$250, police said in a press statement released July 4. Two of the men were arrested without incident at their workplace and a third

surrendered later that day to police. A combination of chemicals was used and when mixed together they become volatile and exploded.

Source:

<http://www.southcoasttoday.com/apps/pbcs.dll/article?AID=/20120705/NEWS/207050349/1018/OPINION>

For another story, see item [45](#)

[\[Return to top\]](#)

## **Agriculture and Food Sector**

27. *July 4, Santa Rosa Press Democrat* – (California; Illinois; New York) **Petaluma dairy recalls cheese under state quarantine order.** Cheese made by Andante Dairy in Petaluma, California, was the subject of a recall and quarantine order announced July 3 by the California Department of Food and Agriculture (CDFA). The recalled cheeses were sold in sizes from 5-8 ounces. The cheeses were sold mainly to retail markets, restaurants, and cheese shops in California, with limited distribution in Chicago and New York. A lack of proper pasteurization could have allowed harmful pathogens to survive in the products, the CDFA warned.

Source:

<http://www.petaluma360.com/article/20120704/COMMUNITY/120709861?Title=Petaluma-dairy-recalls-cheese-under-state-quarantine-order&tc=ar>

28. *July 3, Ag Professional* – (Ohio) **April bee die-off was not due to pesticides, study claims.** A mass die-off of honeybees in April in Ohio was not due to pesticides, according to the Ohio Department of Agriculture, Ag Professional reported July 3. Although the manner in which the bees died suggested they had been poisoned by pesticides, the results did not agree. The department tested samples of dead bees and ran the results against a database of 300 pesticides. However, no pesticides were detected in the samples, according to an agency spokesman. Officials do not know what caused the die-off.

Source: <http://www.agprofessional.com/news/April-bee-die-off-was-not-due-to-pesticides-study-claims-161119395.html>

29. *July 3, U.S. Food and Drug Administration* – (California) **Recalling due to undeclared eggs.** Fruiti Pops, Inc. recalled 178 dozen Fruiti Pops 4-ounce Classic Coconut frozen dessert bars because they may contain egg yolk, the U.S. Food and Drug Administration reported July 3. Fruiti Pops Classic Coconut frozen dessert bars were distributed in Southern California and were sold by push cart vendors and ice cream trucks. These products were distributed between June 25 and June 28. The recall was initiated after it was discovered this product was produced with egg yolk and did not reveal the ingredient on the packaging.

Source: <http://www.fda.gov/Safety/Recalls/ucm310638.htm>

30. *July 3, U.S. Food and Drug Administration* – (National; International) **Voluntary recall of LabDiet and Mazuri feed products.** PMI Nutrition International initiated a

voluntary recall of four varieties of LabDiet and Mazuri feed products due to the potential for an elevated vitamin D level in these products, the U.S. Food and Drug Administration reported July 3. Elevated vitamin D levels can be harmful to animals if fed for extended periods. The products were manufactured at the Richmond, Indiana feed plant and were distributed throughout the United States and to a few international customers. The affected products include: Guinea Pig Diet; Mazuri Small Bird Maintenance; Mazuri Primate Maintenance Biscuit; and Mazuri Maned Wolf Diet. The recall was initiated after the company received a small number of customer complaints, which involved animal illness and small bird mortality.

Source: <http://www.fda.gov/Safety/Recalls/ucm310630.htm>

31. *July 3, Associated Press* – (Tennessee) **Tenn. crops, livestock in peril as drought spreads.** A hot start to summer coming at the end of a spring that was short on rainfall has damaged Tennessee crops and made livestock production harder, the Associated Press reported July 3. The report from the U.S. Department of Agriculture released the week of July 2, listed 94 percent of the State's cropland short or very short on topsoil moisture. According to the report, almost half the corn Statewide is rated in very poor or poor condition with two-thirds of the pastures in this same category. Soybean, tobacco, and cotton acreage remained in mostly fair-to-good condition, but declined substantially in 1 week. Some farmers were hauling water to livestock as springs failed and ponds dried up. They are also having to feed hay early.

Source: <http://www.businessweek.com/ap/2012-07-03/tenn-dot-crops-livestock-in-peril-as-drought-spreads>

32. *July 3, Agence France-Presse* – (International) **China reports bird flu outbreak.** Authorities in China's remote northwestern region of Xinjiang culled more than 150,000 chickens following an outbreak of bird flu, officials said. The outbreak of the H5N1 strain of avian flu initially killed 1,600 chickens and sickened about 5,500, the agriculture ministry said July 2. In an effort to contain the disease, agricultural authorities quarantined the area and culled 156,439 chickens, according to the ministry. The outbreak occurred June 20 but was only confirmed as H5N1 bird flu July 2. The ministry said the outbreak happened at a farm run by the Xinjiang Production and Construction Corps. China is considered one of the nations most at risk of bird flu epidemics because it has the world's biggest poultry population, and many chickens in rural areas are kept close to humans.

Source:

<http://www.google.com/hostednews/afp/article/ALeqM5iPIMCXigI97QkMnK4c9ZcLO6FTIA?docId=CNG.6570597d3c3999dd02f1b742aba26d6c.251>

For another story, see item [6](#)

[\[Return to top\]](#)

## **Water Sector**

33. *July 5, WIBW 13 Topeka* – (Kansas) **Boil order for Rural Water District #2.** A boil warning has been put in place for Osage County, Kansas residents, WIBW 13 Topeka

reported July 4. Officials said it was due to a water main break in Rural Water District #2. Officials said Osage County residents should boil their water as a precautionary measure until further notice, which officials said will likely be July 5 at the earliest.

Source:

[http://www.wibw.com/home/headlines/Boil\\_Order\\_For\\_Rural\\_Water\\_District\\_2\\_161352835.html](http://www.wibw.com/home/headlines/Boil_Order_For_Rural_Water_District_2_161352835.html)

34. *July 5, WDAF 4 Kansas City* – (Missouri) **Water use restricted as problems continue in metro cities.** A Raytown, Missouri boil order was lifted July 5 after low water pressure in the area made officials concerned about contamination. In Lee's Summit, residents remained under a mandatory water restriction. Officials were concerned water storage levels were getting too low after 26 hours without any water from Kansas City, Missouri, due to a pump failure. Lee's Summit was only able to replenish half of its supply, and a water main break in Kansas City was limiting the supply further.

Source: <http://fox4kc.com/2012/07/04/water-use-restricted-as-problems-continue-in-metro-cities/>

35. *July 5, KCTV 5 Kansas City* – (Missouri) **Water main break causes outage, headaches in Independence.** Water service returned July 5 for hundreds of Independence, Missouri residents who went without July 4 due to six water main breaks in the city. A water main break caused problems in the area of Highway 24 and Highway 291, and in Hawthorne Place many residents suffered with low water volume most of the day and none at all during the 2.5 hours while the water department replaced the split main. The water department's distribution manager prioritized repairs based on the size of the main. Officials were not sure what caused the breaks, but noted the heat or heavy usage as possible causes. The department planned to investigate after repairs were complete.

Source: <http://www.kctv5.com/story/18955029/water-main-break>

36. *July 5, KCBD 11 Lubbock* – (Texas) **Groundwater infiltration damages SW Lubbock water system.** Lubbock, Texas was trying to fix a pump station that provides 12 million gallons of water per day to parts of South and West Lubbock, KCBD 11 Lubbock reported July 5. For the second time in several years, the station was damaged by an infiltration of groundwater. The ground storage reservoir was demolished and rebuilt once before. Public records released July 3 said, "The pump building experiences constant groundwater infiltration resulting in damage to the floor. Seepage through concrete joints and cracks in the floor is continuous." The pump bases are 22 feet below the ground. The city set aside \$200,000 for an engineering study to determine the extent of the damage and come up with ways to fix it. Pump Station 10 is already connected to the Lake Alan Henry project, which should come on line sometime in 2012.

Source: <http://www.kcbd.com/story/18956231/groundwater-infiltration-damages-sw-lubbock-water-system>

37. *July 4, WSLs 10 Roanoke* – (Virginia) **Boil water notice for part of Franklin Co.** The Franklin County Health Department and the Virginia Department of Health issued a boil water notice for Highland Lake Waterworks customers, WSLs 10 Roanoke

- reported July 4, because of the power outage from the storms. The outage caused the water supply to be depleted and required water hauling to maintain water service.  
Source: <http://www2.wsls.com/news/2012/jul/04/boil-water-notice-franklin-co-ar-2033592/>
38. *July 4, Lynchburg News & Advance* – (Virginia) **James River showing few adverse signs from Lynchburg sewage spill.** Lynchburg, Virginia, estimated the release of only partially treated sewage June 30 sent about 2.5 million gallons of wastewater into the James River. The discharge lasted about 13 hours as the city's treatment plant struggled with the power outage, preventing it from fully treating its waste. The sewage was disinfected with sodium hypochlorite but did not go through other treatments to filter out solids and other materials. The discharge into the river created a “gray plume” of discoloration that affected about half a mile of the water. The city said it was inspecting the river and had seen no lasting effects, the Lynchburg News & Advance reported July 4. The Virginia Department of Health did not issue any public advisories, but said it is always good to use caution immediately after a sewage discharge or big storm that sends runoff into the river. The city is not at fault for the power failure; both a primary and backup power source were knocked out by the storm.  
Source: <http://www2.newsadvance.com/news/2012/jul/04/james-river-showing-few-adverse-signs-lynchburg-se-ar-2034789/>
39. *July 3, WBIW 1340 AM Bedford* – (Indiana) **32 counties under water shortage warning.** A water shortage warning was issued for 32 counties across Indiana in an effort to inspire voluntary water conservation, WBIW 1340 AM Bedford reported July 3. "This warning phase is still just a voluntary reduction of 10 to 15 percent of water usage, and applies to all different types of water usage in the State," said a spokesperson for the Indiana Department of Natural Resources' Division of Water. Morse Reservoir, Geist Reservoir, and Eagle Creek Reservoir are the primary drinking water sources for Indianapolis, and according to Citizens Water, the levels were dropping daily. While Marion County is not part of the water warning, Citizens asked customers to voluntarily conserve water, and they were warning that there could be mandatory restrictions. The company reported water-usage records June 27-28, and 40 percent of the water was used to water lawns. According to the National Weather Service, Indiana faces a historic drought with no substantial break in the pattern of heat and lack of rain.  
Source:  
[http://www.wbiw.com/state/archives/2012/07/32\\_counties\\_under\\_water\\_shorta.php](http://www.wbiw.com/state/archives/2012/07/32_counties_under_water_shorta.php)
40. *July 3, Associated Press* – (Iowa) **Montour residents asked to boil drinking water.** Residents of Montour, Iowa were asked to boil drinking water July 3 until further notice after a drop in water pressure. The Iowa Department of Natural Resources (DNR) said the drop occurred July 1 after unauthorized use of a fire hydrant. Officials said a resident hooked up a hose to the hydrant to fill a swimming pool. The DNR said unless authorized by the operator of the water system, use of fire hydrants for purposes unrelated to emergencies is not allowed. Montour, southeast of Marshalltown, has 250 residents.



Source: [http://wfcourier.com/news/local/montour-residents-ask-to-boil-drinking-water/article\\_c46e9f1c-c4fa-11e1-8a66-0019bb2963f4.html](http://wfcourier.com/news/local/montour-residents-ask-to-boil-drinking-water/article_c46e9f1c-c4fa-11e1-8a66-0019bb2963f4.html)

For another story, see item [42](#)

[\[Return to top\]](#)

## **Public Health and Healthcare Sector**

41. *July 5, McClatchy Newspapers* – (National) **FDA lays out new system to track medical devices.** July 3, the Food and Drug Administration (FDA) proposed a new system to better track high-risk medical devices after they have gone public, giving patients, doctors, regulators, and consumer advocates access to data about specific products. Every high-risk medical device will be labeled with a unique identification code in an effort the FDA said will improve patient safety. Called a Unique Device Identifier (UDI), the code would provide basic information about the device, such as the name of the manufacturer, the type of device, the model of the device, and an expiration date. It could also include a batch or lot number to help officials better track recalled devices. That data will be stored in a UDI database that is accessible to the public, although no identifying patient information will be included. The FDA plans to phase in the system over 7 years, focusing on the highest-risk medical devices first. Source: <http://www.postbulletin.com/news/stories/display.php?id=1501658>
42. *July 5, KTVI 2 St. Louis* – (Missouri) **Work to repair water main break near Barnes-Jewish continues.** Kingshighway was open in both directions July 5 near Barnes-Jewish Hospital (BJC) in St. Louis following July 4's massive water main break. Emergency management operations were initiated when some of the water from the break got into the basement of Barnes causing a power outage. At least 100 patients were moved and some elective surgeries were postponed. A break in a 12-inch water main in front of the Queeny Tower building sent a muddy river of water across South Kingshighway and eventually into a sub basement of the tower. St. Louis City Water Department workers along with firefighters, police, and Missouri Department of Transportation staff responded. At times the water was more than a foot deep on Kingshighway. A BJC spokesman said firefighters executed a "vertical response" operation to move patients up and down stairs since the elevators were not working. Power was expected to be restored by July 5 and water main repairs completed by late July 6. Source: <http://fox2now.com/2012/07/05/work-to-repair-water-main-break-near-barnes-jewish/>
43. *July 4, WFMZ 69 Allentown* – (Pennsylvania) **Westfield Hospital reopened after unknown chemical forces shutdown.** The Westfield Hospital in South Whitehall Township, Pennsylvania, reopened after an overnight HAZMAT investigation that shut down the building for hours, WFMZ 69 reported July 4. Hazardous materials crews responded after reports that a man entered the building with an unknown chemical on him, officials said. Officials locked the hospital down while crews investigated. The man was sent to another hospital for treatment and was expected to be fine. There was

no word on what the chemical that caused the disruption was, but HAZMAT crews cleared the scene and the hospital was reopened.

Source: <http://www.wfmz.com/news/news-regional-lehighvalley/Westfield-Hospital-reopened-after-unknown-chemical-forces-shutdown/-/132502/15400282/-/15j0a4i-/index.html>

44. *July 3, Fierce Pharma Manufacturing* – (Oklahoma) **FDA warning letter: Oxygen supplier not testing for purity.** For nearly a decade, an oxygen re-filler company may not have tested its products for purity, and the 5-year expiration dates put on labels may be false, according to an FDA warning letter sent to the Norman, Oklahoma plant of Oklahoma Respiratory Care. The June 18 letter, which was posted July 3 on the FDA Web site said inspectors found many shortcomings during their October visit to the plant. Employees said they never received training on how to identify and perform quality inspections on incoming oxygen products, and so never tested them, even though they indicated on batch records they had. A quality control employee said he did not review batch records to see that products met specifications, including 59 lots sold from January through October 18, 2011. A review of records dating back to 2003 provided no proof that any products were tested. Additionally, Oklahoma Respiratory was putting 5-year expiration dates on its products without any stability testing to indicate they would last that long.

Source: <http://www.fiercepharmamanufacturing.com/story/fda-warning-letter-oxygen-supplier-not-testing-purity/2012-07-03>

[\[Return to top\]](#)

## **Government Facilities Sector**

45. *July 4, WTVQ 36 Lexington* – (Kentucky) **Tests on Whitley County substances negative.** Test results are in on two suspicious packages discovered July 3 at a federal facility in Whitley County, Kentucky. The Kentucky Consular Center was closed and three people in the mail room were decontaminated as a precaution. The chief of the Williamsburg Police Department said the State ran several tests on the substances in the packages, and every test for harmful substances has come up negative. He said a few more tests still must be conducted, but it appears it was a scare. The building was closed for the July 4th holiday, but there were some employees inside. The FBI was investigating. The Kentucky Consular Center processes applications for the visa lottery. Source: <http://www.wtvq.com/content/localnews/story/Update-Tests-On-Whitley-County-Substances/WHQK8ovzCk2tyXWV3IwfQA.csp>

46. *July 3, San Francisco Chronicle* – (California) **Officials explain safety calls made during city hall bomb threat.** After San Francisco authorities said they received a bomb threat June 29 targeting City Hall, the mayor's security detail whisked him out of the building, and some of his staff were seen leaving the premises. Other workers and the general public were not told to evacuate. "One of the things we were trying to do was not to induce panic," the building manager said July 3. On a typical day, about 900 employees work at city hall. June 29, the place was buzzing with wedding parties and tourists. The building manager said he made the call not to clear everyone after

consulting with the sheriff's department. The acting sheriff said the information her staff received was that an explosive device was planted outside city hall, perhaps in the hedges or in a car. The building manager said that if there were an explosive device outside city hall, he did not want to put people in harm's way by sending them into a potential danger zone. In consultation with the sheriff's department, he also decided not to lock the building down to keep people inside. The mayor returned to city hall after the all-clear was given when no device was found. The alleged phone threat targeted city hall and the Golden Gate Bridge. Bridge authorities said they rapidly determined the threat was not credible.

Source: <http://blog.sfgate.com/cityinsider/2012/07/03/officials-explain-safety-calls-made-during-city-hall-bomb-threat/>

For another story, see item [11](#)

[\[Return to top\]](#)

## **Emergency Services Sector**

47. *July 5, WNBC 4 New York* – (New York) **Police, FBI investigate hoax 911 calls in Westchester.** Police in Westchester, New York and the FBI were investigating a series of hoax calls that drew heavy police response to nonexistent emergencies over the week of July 2, authorities said. A Rye boy was charged with making a false report, but police believe more people were involved in the hoax calls and may potentially involve a hacking group. The boy was accused only in a June 27 incident, when police received a 9-1-1 call through a typed message using a service for the hearing impaired. Armed police officers arrived at the reported address to find a woman, her teenage son, and two friends. There was no emergency. Rye police are investigating three more hoax calls, dubbed "swatting" because they are meant to draw heavy police response, including from the SWAT team.

Source: <http://www.nbcnewyork.com/news/local/Rye-Hoax-911-Calls-Police-Swatting-False-Emergencies-Arrest-Hacking-161301255.html>

48. *July 3, WBBM 2 Chicago* – (Illinois) **Chicago's 911 system crashes.** Computers were down overnight July 2 into July 3 at Chicago's 9-1-1 dispatch center, after the state-of-the-art system unexpectedly crashed. The system routes emergency calls from the dispatch center to police officers in the field. A spokeswoman for the city's office of emergency management and communications told the Sun-Times Media Wire the system went down for about 4 hours. During the outage, dispatchers manually directed officers to emergencies through their radios. Technicians were working at the center July 3 trying to figure out the cause and make repairs.

Source: <http://chicago.cbslocal.com/2012/07/03/chicagos-911-system-crashes/>

49. *July 3, Washington Post* – (Virginia) **N.Va.'s 911 emergency call system restored, officials say, but questions linger.** Northern Virginia's 9-1-1 system was fully restored after a series of outages and glitches caused by a major storm on the weekend of June 30, a Verizon spokesman said July 3. However, even as the service came back online, area officials raised new questions about how the carrier handled the outage. The

director of Fairfax County's emergency communications center said it took Verizon roughly 3 hours to officially notify the county that 9-1-1 was down after the emergency line went out early June 30. The 9-1-1 problems in Fairfax, Prince William, Arlington, Manassas, and other areas angered local officials and forced residents to call non-emergency lines and even travel to fire stations to get help. The storm knocked out 9-1-1 in a handful of areas beginning the night of June 29. Service began being restored by June 30 afternoon, but problems persisted through July 3. The chairman of the Fairfax County Board of Supervisors and other local leaders said they want a task force formed to investigate the 9-1-1 problems, calling it unacceptable for the system to go out during a major emergency.

Source: [http://www.washingtonpost.com/local/crime/911-emergency-call-system-is-repaired-after-storm-officials-say/2012/07/03/gJQAreq6KW\\_story.html](http://www.washingtonpost.com/local/crime/911-emergency-call-system-is-repaired-after-storm-officials-say/2012/07/03/gJQAreq6KW_story.html)

50. *July 3, Chicago Tribune* – (Illinois) **Hacker may have targeted Lemont's tornado sirens.** Lemont, Illinois police suspect someone hacked into the village's tornado siren system, causing all seven sirens to sound for about 30 minutes, the police chief said July 3. Three sirens were activated inexplicably in Evanston June 30, including two at fire stations, officials said. "Those sirens can only be triggered by our 911 dispatch center," said the city's division chief of life safety services. "It's not something that just anyone can do. We're not certain on the source."

Source: [http://articles.chicagotribune.com/2012-07-03/news/chi-police-hacker-lemont-tornado-siren-20120703\\_1\\_tornado-sirens-sound-warning-radio-signal](http://articles.chicagotribune.com/2012-07-03/news/chi-police-hacker-lemont-tornado-siren-20120703_1_tornado-sirens-sound-warning-radio-signal)

For more stories, see items [14](#) and [61](#)

[\[Return to top\]](#)

## **Information Technology Sector**

51. *July 5, Help Net Security* – (International) **Phonebook-slurping, spam-sending app found in App Store.** A malicious application that steals mobile users' phonebooks and uploads them to a remote server was spotted on Google Play and Apple's App Store. Kaspersky Lab researchers first thought they were detecting an SMS worm, but after analyzing the "Find and Call" app, they discovered it was a trojan. It asks for permission to access user contacts. Once the phonebook is exfiltrated to the server, SMS spam messages containing a link to a page where the free app can be downloaded are sent to all the contacts, inviting them to use it to reach the sender. "It is worth mentioning that the 'from' field contains the user's cell phone number. In other words, people will receive an SMS spam message from a trusted source," said the researchers. "Malware in the Google Play is nothing new but it's the first case that we've seen malware in the Apple App Store," they noted. The Web site of this app allows users to supposedly access their social network accounts, mail accounts, and even their PayPal account. However, by adding money to the PayPal account, they are actually transferring it to a company based in Singapore, Malaysia. Both Google and Apple were notified and removed the app from their markets.

Source: [http://www.net-security.org/malware\\_news.php?id=2174&utm\\_source=feedburner&utm\\_medium=feed](http://www.net-security.org/malware_news.php?id=2174&utm_source=feedburner&utm_medium=feed)

[d&utm\\_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm\\_content=Google+Reader](#)

52. *July 5, Inquirer* – (International) **Sophos discovers an Android spam botnet.** Security firm Sophos discovered Android malware that generates money for cyber criminals by running as a spam botnet. The malware, which is thought to come from downloading pirated programs from unofficial app stores, takes advantage of compromised devices by sending adverts for fake pills such as discounted Viagra and diet tablets, worthless penny stocks, and dubious electronic greeting cards. "The messages appear to originate from compromised Google Android smartphones or tablets," a senior security adviser at Sophos Canada said July 5.

Source: <http://www.theinquirer.net/inquirer/news/2189458/sophos-discovers-android-spam-botnet>

53. *July 5, H Security* – (International) **TYPO3 updates close File Uploader vulnerability.** The TYPO3 development team released updates for all currently supported versions of its open source content management system, fixing a number of bugs and closing a security hole in one of the TYPO3 Core components. According to the developers, the JavaScript and Flash Upload Library (swfupload) used in previous versions of TYPO3 did not properly sanitize the "movieName" parameter before calling "ExternalInterface.call()." This vulnerability could have been exploited by an attacker to execute arbitrary code in a browser session and conduct cross-site scripting (XSS) attacks. Versions 4.5.0 to 4.5.16, 4.6.0 to 4.6.9, 4.7.0, and 4.7.1, as well as the 6.0 branch development releases are affected; upgrading to TYPO3 4.5.17, 4.6.10, or 4.7.2 resolves the problem.

Source: <http://www.h-online.com/security/news/item/TYPO3-updates-close-File-Uploader-vulnerability-1632768.html>

54. *July 5, Computerworld* – (International) **Microsoft to patch under-attack XML bug next week.** July 5, Microsoft confirmed it will patch a vulnerability in Windows the week of July 9 that has been exploited by an increasing number of attacks. Initially, experts wondered whether Microsoft would patch the XML Core Services vulnerability in Windows that it first acknowledged June 12, but failed to fix even as attacks leveraging the flaw steadily ramped up.

Source:

[http://www.computerworld.com/s/article/9228828/Microsoft\\_to\\_patch\\_under\\_attack\\_XML\\_bug\\_next\\_week](http://www.computerworld.com/s/article/9228828/Microsoft_to_patch_under_attack_XML_bug_next_week)

55. *July 4, H Security* – (International) **Ransomware threatens to frame user and inform police.** As well as encrypting files on a victim's computer, a new strain of ransomware discovered by security specialist Sophos threatens to contact the police about certain types of files if the system's owner doesn't pay a ransom of \$3,727. When trying to access data that has supposedly been encrypted, users are presented with a message that instructs them to send a unique ID number to an e-mail address — in this case a Gmail or Live address — to obtain a password to unlock their files once they pay the ransom. However, according to a Sophos researcher, the Troj/Ransom-HC trojan also tells users that if they do not pay the ransom within 96 hours, the criminals will send a report to

the police with a "special password" that will unlock files, said to contain spamming software and child pornography. The goal is to scare users into paying them quickly. Source: <http://www.h-online.com/security/news/item/Ransomware-threatens-to-frame-user-and-inform-police-1632338.html>

56. *July 4, H Security* – (International) **DNSChanger victims to lose internet on Monday.** July 9, the FBI will turn off the DNS server that currently intercepts queries from DNSChanger victims. This means users infected with the malware will be almost completely unable to access the Internet normally. Therefore, users are advised to check whether their computers or routers use one of the FBI-listed IP addresses for DNS queries by visiting dns-ok.us. Users can also check their configuration manually by looking for an IP within several address ranges. If an address from one of the ranges is already set as the DNS server on the computer or router, it is infected with DNSChanger. Users can find out where to locate this DNS server information for their particular case using a wizard set up by the eco association. Future DNS queries can be made using servers such as Google's at 8.8.8.8. Source: <http://www.h-online.com/security/news/item/DNSChanger-victims-to-lose-internet-on-Monday-1632475.html>
57. *July 4, Pittsburgh Tribune-Review* – (International) **Lithuanian admits ID theft plot.** July 3, a Lithuanian national admitted in federal court in Pittsburgh to selling data to an undercover FBI agent that could have compromised the personal information of 10,000 people. The man, of Brick, New Jersey, pleaded guilty to selling 39 log-in names and passwords for \$2,000 to the agent in 2008. An assistant U.S. attorney said the man hacked a data-hosting center, a firm that provides individuals and other companies computer space for Web sites, databases, and other information. The company confirmed 32 of the names and passwords would have given someone back-door access to the company's computers and customer data. With that access, someone could have intercepted financial information from online transactions and installed viruses that would have infected other computers, the U.S. attorney said. The Lithuanian, using the identity "Dr. Smurf," offered the log-in credentials for sale through a site called "Dark Market," the U.S. attorney said. The FBI took over the criminal exchange in 2006 and operated it for 2 years to gather information on people buying and selling identity information, he said. The FBI said the Dark Market investigation led to the arrest of 56 people and prevented an estimated \$70 million worth of thefts. Source: <http://triblive.com/news/2145233-74/petrauskas-information-hull-fbi-company-fischer-selling-log-passwords-access>
58. *July 3, IDG News Service* – (International) **Security researchers link second malware program to rogue printing incidents.** A computer worm that propagates by exploiting a 2010 Windows vulnerability is responsible for some of the recent incidents involving network printers suddenly printing useless data, according to security researchers from Symantec. Many companies reported unauthorized printing incidents in recent weeks, prompting antivirus firms to investigate the possible causes. June 21, Symantec reported the rogue printouts were the result of computers being infected with a trojan program called Trojan.Milicenso. However, they have determined the propagation



routine of a separate piece of malware, a worm called W32.Printlove, can cause similar problems, a Symantec researcher said July 2. W32.Printlove infects other computers on the local network by exploiting a remote code execution vulnerability in the Microsoft Windows Print Spooler service patched in September 2010. Identified as CVE-2010-2729, this vulnerability was also exploited by the Stuxnet industrial sabotage worm to spread. The rogue printing behavior can occur when W32.Printlove unsuccessfully attempts to infect a Windows XP computer connected to a shared network printer.

Source:

[http://www.computerworld.com/s/article/9228778/Security\\_researchers\\_link\\_second\\_malware\\_program\\_to\\_rogue\\_printing\\_incidents](http://www.computerworld.com/s/article/9228778/Security_researchers_link_second_malware_program_to_rogue_printing_incidents)

59. *July 3, Softpedia* – (International) **All Carberp cybercriminals arrested, but infection rates still high.** Experts from ESET and Russian firm Group-IB have been closely monitoring the activities of Carberp botnets and their masters. They stated all the cybercriminals involved in these operations were arrested. The number of infected devices declined immediately after each series of arrests. Currently, however, the number of impacted computers is still high. "All the Carberp botnet organizers have been arrested, but our statistics aren't showing a big drop in detections. The Russian region leads as before for Carberp detections and after the arrests it showed a brief dip," said ESET's Security Intelligence team lead.

Source: <http://news.softpedia.com/news/All-Carberp-Cybercriminals-Arrested-but-Infection-Rates-Still-High-278888.shtml>

For more stories, see items [13](#), [16](#), and [17](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [sos@us-cert.gov](mailto:sos@us-cert.gov) or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <https://www.it-isac.org>

[\[Return to top\]](#)

## Communications Sector

61. *July 3, Washington, D.C. Hill* – (National) **FCC examining storm damage to area phone networks after 911 calls failed.** The Federal Communications Commission (FCC) was looking into the damage that the massive storm that swept from the Midwest into the Northeast June 29 caused to wireless and landline phone networks in the mid-Atlantic, the Washington, D.C. Hill reported July 3. As of early July 2, 16 percent of cell towers in West Virginia were still disabled. Nearly 11 percent of Maryland's towers were down, as well as 9 percent in Virginia, and 3 percent in Washington, D.C., according to the FCC. Widespread power outages also caused problems for many 9-1-1 call centers in the region.

Source: <http://thehill.com/blogs/hillicon-valley/technology/236133-fcc-looking-into-damage-to-phone-networks-from-storm>

For more stories, see items [51](#) and [52](#)

[\[Return to top\]](#)

## **Commercial Facilities Sector**

62. *July 5, WJXT 4 Jacksonville* – (Florida) **Motel 6 evacuated after meth lab found.** Two floors of a Motel 6 in Jacksonville, Florida, were evacuated July 5 after police found an active meth lab in one of the rooms. Officers originally responded after motel security called police about a dispute call. As the officers approached, several people ran out of a room, and a hotel security office found a smoking container, said a lieutenant with the Jacksonville Sheriff's Office. A response team consisting of Jacksonville Fire-Rescue, the police bomb squad, and specialized detectives trained to deal with dangerous chemicals were called. Officers said they were searching for the suspects who ran out of the room. This is the third meth lab incident at a local Motel 6 in the past 2 months.  
Source: <http://www.news4jax.com/news/Meth-lab-found-at-Motel-6/-/475880/15408558/-/biua90z/-/index.html>
63. *July 5, Associated Press* – (Missouri) **FBI helping investigate fire at Joplin mosque.** The FBI joined an investigation into the second fire at a Joplin, Missouri mosque in 4 years. The blaze early July 4 burned a 4-by-6-foot section of shingles atop the Islamic Society of Joplin's building. Firefighters extinguished the flames before they could do further damage, authorities said. A fire official of neighboring Carl Junction said a passer-by noticed the fire and called it in. Authorities examined the roof after the fire was out. "We noticed a bunch of what looked like paper up there," the fire official said. "Somebody lit them and threw them up there." The Jasper County Sheriff's Department said they were studying security camera footage. About 50 families are members of the Islamic Society of Joplin, which opened the building in 2007 as a mosque and community center, society officials said. The FBI led an investigation in 2008 when the mosque's sign was torched; that crime remained unsolved.  
Source: [http://www.stltoday.com/news/state-and-regional/missouri/fbi-helping-investigate-fire-at-joplin-mosque/article\\_3efe6172-e664-562e-b2bd-4e2998b9cc6a.html](http://www.stltoday.com/news/state-and-regional/missouri/fbi-helping-investigate-fire-at-joplin-mosque/article_3efe6172-e664-562e-b2bd-4e2998b9cc6a.html)
64. *July 4, KVOA 4 Tucson* – (Arizona) **HAZMAT crew determines downtown building was leaking Freon.** Four Tucson, Arizona firefighters were taken to the hospital July 4 as a precaution after complaining of nausea after responding to a fire alarm at a building downtown. Crews donned protective equipment and headed to the building's basement where the alarm originated, according to a Tucson Fire Department news release. Once smoke was verified, additional units were called in and the building was evacuated. Two four-person crews entered the basement. Two members became nauseated while investigating the smoke. Using special tools including air monitors, hazardous materials crews determined that a chiller in the basement had a broken pipe that was emitting Freon into the air, which caused the appearance of fog. Building representatives were working to fix the broken pipe.

Source: <http://www.kvoa.com/news/hazmat-crew-determines-downtown-building-was-leaking-freon/>

65. *July 4, WPDE 15 Florence* – (South Carolina) **Firefighters respond to hazardous situation.** Firefighters closed down 100-150 feet of the beach near Water Pointe One condos in North Myrtle Beach, South Carolina, because of a hazardous material situation, said the fire battalion chief. Someone improperly mixed together two pool chemicals, muriatic acid and chlorine. There was about 5 gallons of the mixture in drum in the pool area, the fire chief said. Because of an inhalation risk, firefighters closed part of the beach. The Horry County HAZMAT team capped the drum and removed it. The beach was opened July 4.  
Source: <http://www.carolinalive.com/news/story.aspx?id=772658#.TW2Q5GqHU1>
66. *July 4, Associated Press* – (Tennessee) **Leak in heat exchanger blamed for hotel blast.** A June explosion at the Gaylord Opryland Resort and Convention Center in Nashville, Tennessee, was caused by a leak in a heat exchanger allowing natural gas to mix with steam, fire officials said July 3. The Nashville Fire Department ruled the June 19 blast accidental. No one was hurt, though 5,000 guests were forced out for as long as 7 hours. Damage was estimated at up to \$750,000. The fire department said in a statement the mixture led to an explosion caused by equipment failure. The heat exchanger has been sent to an Atlanta laboratory for further testing. The hotel resumed normal operations the day following the blast. Major damage was done to an escalator, walls, and ceiling. Sheriffs from across the country were attending a convention at the sprawling hotel at the time. The hotel, with 2,881 rooms, has 1 million guests annually.  
Source: <http://www.jacksonsun.com/viewart/20120705/NEWS01/307050014/Leak-heat-exchanger-blamed-hotel-blast?odyssey=tab|topnews|text|FRONTPAGE>
67. *July 4, Associated Press* – (Pennsylvania) **Fire displaces 28 in Philadelphia.** Fire investigators were trying to find out what started a three-alarm fire at a Southwest Philadelphia, Pennsylvania garage that spread to adjoining rowhouses, displacing at least 28 people. The fire in the city's Kingsessing section was reported late July 3 and was placed under control within about 90 minutes. Residents reported hearing fireworks in the area before the blaze began. The American Red Cross of Southeastern Pennsylvania said it was providing shelter to 28 people from six families. More than two dozen homes housing as many as 70 people were evacuated as a precaution, officials said. An evacuation center was set up at a nearby school to assist displaced residents.  
Source: <http://www.courierpostonline.com/article/20120705/NEWS01/207050306/Fire-displaces-28-Philadelphia>
68. *July 4, WBZ 4 Boston* – (Massachusetts) **Esplanade evacuated due to threat of severe weather.** The Esplanade was evacuated for nearly a half-hour during the Boston Pops Fireworks Spectacular in Boston due to severe storms in the area July 3. A severe thunderstorm warning was issued in Essex County north of Boston. An announcement came on the P.A. system telling the crowd to seek shelter. Massachusetts State Police troopers ushered the crowd into the Storrow Drive tunnels to wait out the storm. An

estimated 500,000 people were in the area at the time. Shortly after 10 p.m., the crowd was allowed to return. The storm missed the city. A State police spokesman defended the decision saying, “lightning was observed along nearby areas of the Charles River in Boston and in neighboring communities. The decision to evacuate was the prudent one, made in the interest of the safety of the thousands upon thousands of visitors. It was a seamless operation.”

Source: <http://boston.cbslocal.com/2012/07/04/esplanade-evacuated-due-to-severe-storms/>

69. *July 3, Placer Herald* – (California) **Pipe bomb found at shopping center.** An explosive device was discovered July 2 in a parking lot at the corner of Sunset Boulevard and Park Avenue, reported a Rocklin, California police lieutenant. A citizen spotted the suspicious device behind Bank of America and the Arco AM/PM gas station and called Rocklin police. The device, which was made with PVC pipe, was rendered safe by the Placer County Explosive Ordinance Disposal Unit. Responding officers cordoned off a large section of the parking lot and warned neighboring businesses and residents to remain clear of the area. The device was removed for forensic examination at the crime lab, the police lieutenant said.

Source: <http://placerherald.com/detail/212201.html>

For more stories, see items [1](#) and [16](#)

[\[Return to top\]](#)

## **National Monuments and Icons Sector**

70. *July 5, KRZK 106.3 FM Branson* – (Missouri) **Glade Top Trail fire burning up to 1500 acres.** A wildfire burned as much as 1,500 acres of northeastern Taney County, Missouri, in the Glade Top Trail area. A representative of the U.S. Forest Service said it was named the Liberty Fire, and it started July 4 in the Mark Twain National Forest.

Source:

[http://hometowndailynews.com/10956/glade\\_top\\_trail\\_fire\\_burning\\_up\\_to\\_1500\\_acres.html](http://hometowndailynews.com/10956/glade_top_trail_fire_burning_up_to_1500_acres.html)

71. *July 5, KSTU 13 Salt Lake City* – (Utah) **Quail Fire 10 percent contained, more evacuations lifted.** A brush fire in the Highland-Alpine area was threatening homes, according to Utah County Dispatch. The fire started July 3 just south of Lambert Park. As of July 5, there were mandatory evacuations for about 285 homes. However, residents in the Alpine Cove subdivision were allowed home. The Red Cross continued shelter operations at Timberline Middle school in Alpine. The fire was 10 percent contained. State Road 93 starting at the mouth of American Fork Canyon remained closed.

Source: <http://fox13now.com/2012/07/03/brush-fire-threatening-homes-in-alpine-area/>

[\[Return to top\]](#)

## **Dams Sector**

72. *July 5, Victoria Times-Colonist* – (International) **Tailings pond dam leaking after rains.** A local state of emergency was declared in an area of southeast British Columbia, Canada, after a dam holding back a tailings pond for an old lead-zinc mine began leaking, the Victorian Times Colonist reported July 5. The Regional District of Central Kootenay issued the declaration for the Nelson-Salmo area over concerns that part of the retaining wall for the old Hudson's Bay mine tailings pond had been washed away by heavy rains. The regional district's emergency operations center said engineers were working on plans to shore up the dam and many rumors the dam could collapse were exaggerated. Officials said the area downstream from the dam is sparsely populated and the emergency declaration for the area remains in effect.

Source:

<http://www.timescolonist.com/news/Tailings+pond+leaking+after+rains/6887087/story.html>

[\[Return to top\]](#)



**Department of Homeland Security (DHS)**  
**DHS Daily Open Source Infrastructure Report Contact Information**

**About the reports** - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

**Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703)387-2314
Subscribe to the Distribution List:	Visit the <a href="#">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="#">Get e-mail updates when this information changes</a> .
Removal from Distribution List:	Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a> .

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

**Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.